U.S. ARMY SIGNAL CENTER AND FORT GORDON
Fort Gordon, Georgia 30905-5180

LESSON PLAN

TITLE: Introduction to Communications Security (COMSEC)

LEARNING OBJECTIVE:

Action: The student will be able to explain the basic terms and definitions of COMSEC.

Conditions: The students will receive classroom instruction.

Standard: Acceptable performance is met when the student can correctly answer verbal questions given by the instructor.

SAFETY CONSIDERATIONS: There are no safety considerations for this lesson.

RISK ASSESSMENT: Low.

RESOURCE NEEDS/ REFERENCES: Overhead Projector, Slides 1-12, AR 380-5, AR 380-40, and AR 380-41.

METHOD OF INSTRUCTION: Conference.

TIME: 1 Hour

NOTES TO INSTRUCTOR:

1. Explain to students that notes written during class WILL NOT leave the building.

APPROVAL DATE: 24 NOV 97
DEVELOPER: SFC CARTAGENA
DIV. CHIEF: Jack P. Rondon

2. Any notes written during the COMSEC block of instruction will be collected by the instructor at the end of each day and returned to the students for the next class.

3. All COMSEC notes will be collected from each student and destroyed either upon completion of the written exam or when a student leaves the course for any reason.

INTRODUCTION:

1. Whenever “private” or "personal in nature" information is passed on from one individual to another, measures are often taken to ensure that information is provided only to those persons intended to obtain it.

2. Large corporations also go to great extremes to prevent industrial espionage, the stealing of industrial secrets, from occurring.

3. In military communications, the need to prevent the enemy or unauthorized personnel from obtaining information is also of extreme importance. The term for these preventive measures is Communications Security (COMSEC).

4. At the conclusion of this lesson, you will be familiar with various terms and definitions used in practicing COMSEC.

3M

BODY:

1. Preface.

   a. During this lesson, you will be taught the basics of how the Army and the TRI-TAC family of switches secure their communications through the use of encryption and decryption devices.

   NOTE: Show Slide 1.

2. Terms and definitions.

   a. COMSEC.

(1) The protection resulting from all measures designed to deny unauthorized persons information of value, relating to the national security, which might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications.
(2) COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC material and information.

(a) Information - knowledge that can be communicated by any means.
(b) National Security - the national defense and foreign relations of the United States.

(3) Equipment - often throughout the remainder of your career in the signal corps, the term COMSEC will be used to refer not to the "act" of communication security, but to the equipment used to provide for that security.

(a) A KY-68 digital subscriber voice terminal (DSVT) telephone will be referred to as a COMSEC phone.
(b) Various pieces of equipment used to provide communication security will be referred to as COMSEC devices.

(4) There are two basic types of COMSEC; physical and equipment oriented.

(a) Physically-oriented COMSEC.

1. This form of COMSEC involves the physical security of the transmission path over which the intelligence is being transmitted.
2. Various cable systems and subscribers may be determined to be or classmarked "secure" even though the equipment they

are using is not a COMSEC device.

NOTE: Show Slide 2.

3. In this type of application, the phone must be located inside a secure area. The line between the phone and any type of junction box, and the cable to the switch must be guarded by an armed roving guard.
4. The major problem with this type of communication security is the possibility of human error.

(b) Equipment oriented COMSEC.

1. For the most part, this is the "meat" of the term COMSEC.
2. This equipment makes up the group of devices that perform all of the encryption and decryption services for the TRI-TAC subscribers.
3. The equipment provides for the COMSEC. The operator or subscriber does not have to ensure that the cables and lines are physically guarded.
4. The various devices that you have been introduced to at the beginning of the course will be explained in-depth during this portion of the course.

b. Compromise.

The disclosure of classified information to persons not authorized access thereto.

c. Classified information.

(1) Information or material that is owned by, produced for or by. or under control of the US Government.

(2) Information or material that is determined to require protection against unauthorized disclosure and so designated.

Material - any product or substance on, or in which, information is embodied.

d. Classification authority.

The authority vested in an official of the Department of Defense (DOD) to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

NOTE: Show Slide 3.

e. Security classification designations.

Information or material that has been determined to require protection against unauthorized disclosure in the interest of national security shall be classified in one of three designations: TOP SECRET, SECRET, or CONFIDENTIAL.

NOTE: Show Slide 4.

(1) TOP SECRET.

(a) Applied only to information or material the unauthorized disclosure of which could be exceptionally grave damage to the national security.

15M

(b) Examples of exceptionally grave damage:

1. Armed hostilities against the US or its allies.
2. Disruption of foreign relations vitally affecting the national security.

3. The compromise of vital national defense plans or complex cryptologic (manner in which characters are substituted or transposed into code) and communications intelligence systems.
4. The revealing of sensitive intelligence operations and the disclosure of scientific or technological developments vital to national security.

NOTE: Show Slide 5.

(2) SECRET.

(a) Applied only to information or material the unauthorized disclosure of which could be expected to cause serious damage to the national security.
(b) Examples of serious damage.

1. Disruption of foreign relations significantly affecting the national security.
2. Significant impairment of a program or policy directly related to the national security.
3. The disclosure of significant military plans or intelligence operations or the compromise of said plans or operations.
4. The compromise of significant scientific or technological developments relating to national security.

NOTE: Show Slide 6.

(3) CONFIDENTIAL.

(a) Applied only to information or material the unauthorized disclosure of which reasonably

could be expected to cause damage to the national security.

(b) Examples of identifiable damage.

1. Compromise of information that indicates the strength of ground, air, and naval forces in the US and overseas areas.
2. Disclosure of technical information used for training, maintenance, and inspection of classified equipment.
3. The revealing of performance characteristics, test data, design, and production data on equipment.

(4) The markings FOR OFFICIAL USE ONLY and LIMITED OFFICIAL USE shall not be used to identify classified information.

NOTE: Show Slide 7.

f. Classification authority.

The authority vested in an official of DOD to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

(a) Original classification authority.

Authority for original classification of information as TOP SECRET, SECRET, or CONFIDENTIAL may be exercised only by the Secretary of Defense, the Secretaries of the Military Departments, and by officials to whom such authority is specifically delegated.

(b) Delegated classification authority.

1. Original TOP SECRET classification authority can

only be delegated by those persons who have original TOP SECRET classification authority.

2. Original SECRET and CONFIDENTIAL classification authority can only be delegated by those persons who have original TOP SECRET classification authority.

NOTE: Show Slide 8.

g. Classification guidelines.

(1) Compilation of information.

Certain unclassified information when combined or associated with other unclassified information may provide an additional factor that would warrant the classification of the combined information.

(2) Extracts of information.

(a) Information extracted from a classified source shall be derivatively classified or not classified in accordance with the classification markings shown in the source.

(b) If internal markings of the source of information (paragraph e) are not adequately marked, the extracted information shall be classified according to the overall marking of the entire source.

h. Custodian.

An individual who has possession of or is otherwise charged with the responsibility for safeguarding or accounting for classified information.

i. Declassification.

(1) The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure.
(2) The removal or cancellation of the classification designation would be made to the declassified information.

j. Up/Down grading of classification.

A determination that certain classified information requires, in the interest of national security, a higher or lower degree of protection against unauthorized disclosure than currently provided, together with the changing of the classification designation to reflect such higher or lower degree.

k. Document.

(1) Any recorded information regardless of its physical form or characteristics including without limitation.
(2) Written or printed matter, data processing cards and tapes, maps, charts, paintings, drawings, engravings, sketches, working notes and papers, reproductions of such things by any means or process, and sound, voice, magnetic or electronic recordings in any form.

NOTE: Show Slide 9.

l. Controlled cryptographic items (CCI).

(1) A secure telecommunications or information handling equipment ancillary device, or associated cryptographic component, which is unclassified but controlled.
(2) Equipment and components, so designated, bears the designator "Controlled Cryptographic Item" or "CCI".
(3) If the device, such as a KYK-l3 is labeled "CCI", that only applies if it

contains NO keys. Whenever loaded with keys, the device "assumes" the classification of the keys within.

QUESTIONS: The term COMSEC refers only to equipment used to prevent unauthorized persons from obtaining information of value, true or false? (ANS: False, applies to any measure taken to protect information.)

How many levels of classification are there? (ANS: Three; Top Secret, Secret, Confidential.)

An item of COMSEC labeled CCI never has a level of classification applied to it, true or false? (ANS: False, when loaded with a key, it carries the level of classification as the key it contains.)

35M

3. Application to AN/TYC-39A.

a. Overview.

(1) Army regulations state that if classified material is to be passed over a transmission system it must be coded, encrypted, or the circuits must be physically protected from compromise.
(2) Protection systems must meet the standards specified by the National COMSEC and Emanation Security Insurance System.
(3) Cryptographic systems must be approved by the Director, National Security Agency (NSA).

NOTE: Show Slide 10.

b. Terms and definitions.

(1) Plain text - traffic on a circuit that is non-encrypted (not encoded).
(2) Cipher text - traffic on a circuit that has been encrypted (encoded).

(3) Key or key stream - a random bit pattern of 128 bits used to encode traffic on a circuit.

NOTE: In the past, many telecommunications personnel have used the term "variable" to indicate an electronic key. It is now preferred that the term variable no longer be used and the term "key" be used exclusively.

(4) Crypto key - a stream of bits that controls the pattern of the key stream.
(5) Red (traffic) - refers to a circuit on which the traffic has not been encrypted or encoded.
(6) Black (traffic) - refers to a circuit on which the traffic has been encrypted or encoded.

45M

NOTE: Show Slide 11.

4. Emission security.

a. Emission security is that component of COMSEC which is concerned with any measures taken to deny unauthorized persons information of value that might be derived from the interception and analysis of compromising emanations.

b. Compromising emanations - unintentionally transmitted data related, or intelligence-bearing signals.

(1) A compromising emanation exists when electromagnetic energy is unintentionally emitted from equipment that is processing classified information.
(2) The radiation itself can be intercepted and analyzed, causing classified information to be exposed and recovered by the wrong people.

c. TEMPEST - a term often used as a synonym in place of compromising emanations.

d. TEMPEST prevention in joint tactical communications (TRI-TAC) switching.

NOTE: Show Slide 12.

(1) By now you may have noticed that the AN/TYC-39A has a unique gasket surrounding the port hole in the shelter door, as well as, the shelter door itself.

(a) These are special purpose gaskets called electromagnetic interference (EMI) gaskets.
(b) EMI has an appearance of woven metallic fibers that are designed to retard electromagnetic emanations.

(2) The emergency exit, battery exhaust vent and personnel comfort fan vent openings are protected by a "honeycombed" screen. These "honeycombed" openings are designed so that the hexagonal shape and the volume are combined to create a resonate cavity which absorbs the electromagnetic emanations which are constantly being created within the switch.

(3) All of these devices are designed to keep the emissions created during normal operation of the switch "inside" the switch and away from the ears of the enemy.

(4) Sources of compromising emanations within the switch.

(a) Visual display terminal (VDT) keyboard.
(b) DFDD.
(c) Line printer unit (LPU).
(d) Normal digital traffic in plain-text mode.

e. To ensure that classified information is not compromised by the unauthorized interception of emanations from information processing equipment, the switch operator must ensure

that the protective devices designed into the switches can perform their functions by replacing worn gaskets and keeping the door closed when processing traffic.

QUESTIONS: Define EMI. (ANS: Electromagnetic interference.)

What term is often used in place of emission security? (ANS: TEMPEST.)

Name three devices inside the switch that produce compromising emanations. (ANS: VDT keyboard, DFDD, LPU, or normal digital traffic in plain test.)

NOTE: Show Slide 10. Use for review questions if time permits.

55M

SUMMARY:

During this lesson, you were introduced to COMSEC, classification procedures, and a few of the commonly used terms. You were showed a simplified version of how voice/data traffic is encrypted and decrypted. You were introduced the concept of TEMPEST hazards and how to prevent them. These principles will be applicable throughout your career.

1H

END

This document supports Task Number 113-603-3205.

U.S. ARMY SIGNAL CENTER AND FORT GORDON
Fort Gordon, Georgia 30905-5180

LESSON PLAN

TITLE: Functional Analysis of COMSEC Equipment

LEARNING OBJECTIVES:

Action: The student will describe the general purposes and identify common names of the COMSEC equipment used in AN/TYC-39A switch applications.

Conditions: The student will be given: CONFIDENTIAL manuals FM 24-27A and KAO-193A/TSEC; FOUO TMs 11-5810-258-12, 11-5810-256-OP-5, 11-5810-292-13&P, 11-5810-309-10, 11-5810-323-12, 11-5810-326-13, 11-5810-329-10, 11-5810-330-13, 11-5810-331-13, and 11-5810-381-10; and practical exercise.

Standard: Acceptable performance is achieved when the student correctly answers 14 out of 20 questions.

SAFETY CONSIDERATIONS: There are no safety considerations for this lesson.

RISK ASSESSMENT: Low.

RESOURCE NEEDS/ REFERENCES: CONFIDENTIAL manuals FM 24-27A and KAO-193A/TSEC; FOUO TMs 11-5810-258-12, 11-5810-256-OP-5, 11-5810-292-13&P, 11-5810-309-10, 11-5810-323-12, 11-5810-326-13, 11-5810-329-10, 11-5810-330-13, 11-5810-331-13, 11-5810-381-10; practical exercise, overhead projector, and slides 1-15.

METHODS OF INSTRUCTION: Conference, Practical Exercise.

APPROVAL DATE: 24 NOV 97
DEVELOPER: SFC CARTAGENA
DIV. CHIEF: Jack P. Rondon

TIME: 4 Hours

NOTES TO INSTRUCTOR:

The blank practical exercise (PE) is not classified; however, when the student completes any portion of the PE, the PE is considered CONFIDENTIAL.

INTRODUCTION:

Elapsed Time

1. As described in the previous lesson, the basic purpose of COMSEC equipment is to deny vital intelligence to the enemy.

2. During this lesson we will identify the equipment used in the message switch, applications in joint tactical communications (TRI-TAC) and MSE networks. We will discuss the operations and functions of this equipment. The knowledge you obtain from this lesson will assist you in the future when interfacing with other systems using some of the same type of equipment.

3M

BODY:

1. COMSEC capabilities – TRI-TAC.

   a. COMSEC provides for encrypted secure communications for voice and data traffic between subscribers with compatible equipment via

      (1) Loops.
      (2) Trunks.
      (3) Engineer orderwire (EOW).

   b. In MS applications COMSEC equipment provides for generating, assigning, distributing, and verifying of keys used in a secure network. The switch processor controls electronic key generation and transfer. Keys may also be transferred through manual control of the operator.

   c. The COMSEC equipment ensures that only properly loaded keys and programmed

instruments can access the secure network capabilities.

d. COMSEC equipment provides for encryption/decryption of keys.

NOTE: TRI-TAC is in a transitional state of using the term key instead of "variable". Some references will still use but the term key should be possible.

QUESTION: Besides subscriber loops and trunks, for what else does the COMSEC equipment in the circuit switch provide encryption/decryption capabilities? (ANS: EOW.)

8M

2. COMSEC equipment functional description.

NOTE: Refer to TM 11-5810-292-13 (FOUO) and KAO-193A/TSEC (C).

a. Fill devices: General purpose tape reader, KOI-18/TSEC; electronic transfer device (ETD) KYK-13/TSEC; and net control device (NCD) KYX-15/TSEC. The devices are controlled cryptographic items (CCI).

(1) The purpose of these small, portable fill devices is to store, transfer, and/or receive keys to/from compatible COMSEC equipment or from one fill device to another. The National Security Agency (NSA) has directed that a fill cable be connected to the fill device when transferring a key.

NOTE: Show Slide 1.

(2) KOI-18 tape reader, general purpose.

(a) Battery operated, hand-held device.
(b) Converts eight-level standard paper and mylar tape to serial electronic information.
(c) Loads keys from prepunched tape to other COMSEC equipment, KYK-13 or KYX-15.
(d) Has no storage capability.

(e) Tapes are normally generated ahead of time and stored for later use. May be distributed by mail or courier.
(f) Controls and indicators: explain locations and functions using TM 11-5810-292-13, para 2-1.

NOTE: Show Slide 2.

(3) KYK-13 - electronic transfer device.

(a) Battery operated, hand or pocket carried device.
(b) Supplied with lanyard to place around user's neck to prevent loss of device.
(c) Provides for transfer and storage of up to six keys.
(d) Can transfer keys to KYK-13, KYX-15, or to other compatible COMSEC equipment,
(e) Can receive keys from KOI-l8, KYK-18, and other compatible COMSEC equipment.
(f) Has a writing surface to identify keys in storage areas.
(g) Controls and indicators: explain locations and functions using TM 11-5810-292-13 (FOUO), para 2-2.

NOTE: Show Slide 3.

(4) KYX-l5 - net control device.

(a) Battery operated.
(b) Provides for transfer and storage of up to 16 keys.
(c) Can transfer keys to KYK-13, KYX-15, or other COMSEC equipment.
(d) Can receive keys from KOI-18, KYK-13, KYX-15, and other COMSEC equipment.
(e) Can be used for over-the-air rekey (OTAR) operation for both transmitting and receiving keys from another KYX-15 through either a KY-57 or KY-88.

(f) Has a writing surface to identify keys in storage areas.
(g) Controls and indicators - explain locations and functions using TM 11-5810-292-13 (FOUO), para 2-3.

QUESTION: Which of the fill devices is not capable of storing keys? (ANS: KOI-l8 tape reader.)

NOTE: Show Slide 4. Refer to TM 11-5810-328-13 (FOUO) and KAO-193A/TSEC (C).

b. Interface control unit (ICU) HGX-84/TSEC - CCI.

(1) A signaling buffer unit that provides interface for status and control between COMSEC equipment and switch processor via the COMSEC controller. The COMSA card of the COMSEC controller is primarily used for the HGX-84. These interfaces include:

(a) Clock signals.
(b) Status request and reports.
(c) Error signals.
(d) Control (command) signals.
(e) Alarm signals.

1. Rack overtemp condition.
2. Indicator device alarm.
3. Circuit breaker operation to detect alarm conditions.

(2) Redundant configuration - One HGX-84 operates in on-line mode. Any ICU can talk to either switch processor. COMSEC operation is possible with only one HGX-84.
(3) Controls and indicators - explain locations and functions using TM 11-5810-28-13 (FOUO), para 2-2.

(a) POWER ON/OFF switch.
(b) POWER indicator.
(c) ON-LINE indicator.
(d) Circuit breaker.
(e) OVERTEMP indicator.

NOTE: Show Slide 5. Refer to TM 11-5810-331-13 (FOUO) and KAO-193A/TSEC (C).

c. Key variable generator, KVG or KG, TSEC/KG-83. Classification determined by certification level. (SECRET for school, TOP SECRET for field.)

(1) Generates a 128-bit random-bit pattern key. It has been said that this pattern would not be repeated in over 100 years. In TRI-TAC application, the KVG can be used to generate keys under switch processor request or operator manual request.

(a) Manual application - generates and transfers a key to a fill device connected to a KVG front panel connector. The operator presses the INITIATE pushbutton on the fill device. In this application the KVG can be off-line or on-line.

(b) Dedicated application - operates on-line with a dedicated automatic key distribution center (AKDC). Upon command from the switch processor, electronically generates and transfers keys to the dedicated AKDC via rear transition plate assembly.

(2) Follows operational state of dedicated AKDC. Will go to on-line state when associated AKDC is on-line.

(3) Lowest level of classification is CONFIDENTIAL. In the field environment the KG-83 must be certified before being used to pass live traffic. Certification will depend on level of traffic to be processed. Normally it is certified SECRET in CS application; TOP SECRET in MS application. Generally, the KG-83 must be stored in a COMSEC vault when not in use.

(4) Controls and indicators - explain locations and functions using TM 11-5810-331-13, para 2-2.

QUESTIONS: The HGX-84s are dedicated to the processors and are not redundant. True or false? (ANS: False.)

What device generates keys for use by the AKDC? (ANS:KG-83.)

NOTE: Show Slide 6. Refer to TM 11-5810-327-10 (FOUO) and KAO-l93A/TSEC (C).

d. Automatic key distribution center/rekeying control unit (AKDC/RCU) HGX-83/TSEC (C) or HGX-83A/TSEC (C) - lowest classification is CONFIDENTIAL.

(1) The AKDC operates in a slave mode (on-line) to the circuit switch processor. The AKDC provides for storage of keys transferred from fill devices and under processor control to other COMSEC equipment. The hardened unique storage (HUS) of the AKDC provides locations for the long term storage of these keys.

NOTE: Advise students that they will also hear hardened unique storage for HUS.

(2) The HUS memory storage is accomplished by utilizing individual iron ferrite cores (doughnuts) for each bit of information. This enables the HUS to retain keys when power is removed. This HUS design also protects rekey keys from alteration as the result of exposure to an electromagnetic pulse (EMP) occurrence, such as an explosion of a nuclear device.

(3) The HUS contains 1024 (1K) memory locations. Keys that are read into or from these locations are encrypted/ decrypted by the "Z" key.

(a) The Z key protects keys from compromise in the event of an overrun situation.

1. If given enough time, the operator can open the code changer door on the AKDC front

panel to zeroize the “Z” key. The contents of the HUS are unchanged but no keys can be accessed in the AKDC without reloading the proper “Z” key (normally stored in a safe in another area).

2. If the operator doesn't do the above and the enemy tries to remove a properly installed AKDC from the rack, the code changer door will have to be opened and the “Z” key will be zeroized. To remove the AKDC the code changer door must be opened to access a mounting screw. When installing the AKDC in the rack, failure to use all mounting screws is a COMSEC violation.

(b) The 1024 memory locations are addressed and used as follows:

1. Addresses 0000 through 0299 - storage locations for rekey keys (KEK - keys that encrypt traffic keys).
2. Addresses 0300 through 0599 - storage locations for traffic keys (TEK - keys that encrypt voice or data traffic).
3. Addresses 1008 through 1022 - scratch pad store (SPS) or momentary memory. The keys placed in SPS are only permitted to be read out to set up one call, either to a single DSVT, between two DSVTs, or in a conference involving multiple DSVTs.
4. Address 1023 - used in HGX-83 diagnostics (command 89) .
5. Normally not all 1024 memory locations will be needed for keys used in CS/MS operation. The extra locations can be used to store keys that are not used in call set up

procedures (for example, trunk teed keys).

(4) The operator can perform manual commands by using the front panel controls to access HUS locations and perform specific functions with the keys. These commands are (see table on next page).

(5) In the MS operation the HGX-83 does not provide the automatic key distribution feature to transfer keys to terminals. The HGX-83 in the MS does not operate under processor control. It functions in an off-line mode. HUS storage locations are accessed manually or by the rekeying control feature of the HGX-83. Keys are transferred electronically to the HUS using command 91; however, most of the keys that will eventually be used in the net are pregenerated and loaded from a fill device into the HGX-83. The keys are then transferred from the HUS to the dedicated KG-82 using a fill device and KG-82 mode switch on the HGX-82.

NOTE: Show slide 7. Refer to KAO-l93A/TSEC (C),para 1005.b for control and indicator explanations.

(6) Controls and indicators - give a brief description of the following:

(a) Manual mode controls.

1. COMMAND/ADDRESS switches.
2. FUNCTION switches.

a. CMD.
b. ADRS A - used with a command to indicate one address or first address.
c. ADRS B - used with a command that requires a second address.

3. START pushbutton.
4. LAMP TEST pushbutton.
5. POWER circuit breaker.

6. Z FILL Switch.

(b) Indicators.

1. Yellow ADRS A indicator.
2. Yellow ADRS B indicator.
3. Yellow CMD NO indicator.
4. Red ERROR indicator.
5. Red BAT LOW indicator.
6. DISPLAY.
7. Alarms.

a. OVERTEMP indicator.
b. HUS indicator.
c. CRYPTO indicator.
d. Z ZERO indicator.

8. ON-LINE indicator.
9. DPE (display parity error) indicator.
10. Power.

a. HUS ON indicator.
b. POWER ON indicator.

(c) Battery compartment: Area for a storage battery for the "Z" key.

(d) FILL connector: Allows a fill device to be connected to perform various transfers of keys.

QUESTIONS: What is the purpose of the scratch pad storage? (ANS: Temporary storage of keys used to set up secure calls.)

What is the purpose of the "Z" key? (ANS: To protect the contents of the HUS from compromise in the event of an overrun situation.)

When does the AKDC operate in an OFF-LINE mode? (ANS: In MS applications.)

NOTE: Show Slide 8. Refer to TM 11-5810-326-13 (FOUO) and KAO-l93A/TSEC (C).

e. Loop key generator/common unit (LGK/CU), HGX-82/TSEC-CCI.

(1) Contains all electronics common to a group of up to eight KG-82s. Provides:

(a) Power.
(b) Signal buffering and interface for commands, clock, and status between KG-82s and HGX-84.
(c) Interface for transfer of keys to/from HGX-83 and KG-82.
(d) Transfer keys to KG-82 by use of a fill device.
(e) Permits selection of KG-82 operate and rekey modes.
(f) Monitors alarm functions. Provides alarm signal to HGX-84 when alarm condition occurs.
(g) Storage battery to hold KG-82 keys and initialization data in the event of a power failure.

(2) Commands sent to a KG-82 in a group are decoded in the HGX-82 which then activates the designated KG-82's command logic.
(3) Controls and indicators - explain locations and functions using KAO-l93A/TSEC (C), para 1003.d or TM 11-5810-326-13, para 2-2.

(a) KG-82 MODE rotary switch - selects one of five operations when used with KG-82 MODE INIT button.

1. LAMP TEST position - activates BUSY and ALARM lights on associated KG-82s.
2. LDU position - allows a key transfer from a fill device to a selected KG-82 storage location.

a. In MS operation the position is used during initialization and during use of a KG-82 that if required to terminate a trunk between the MS and the CS. Allows loading of key to a dedicated KG-82.

3. LDX position - allows a key transfer from a fill device to a selected KG-82 storage location.

a. In MS operation LDX is used during initialization and to load a new variable when needed (manual load).

4. OP position - normal operating position.
5. RK position - Used in MS for manual rekeying of a MS subscriber terminal.

(b) HGX-82 LAMP TEST pushbutton - illuminates the lights on the HGX-82.
(c) ENABLE/ZEROIZE locking type toggle switch used to zeroize all keys stored in all KG-82s connected to the HGX-82.
(d) POWER toggle switch - controls power input to the HGX-82 and in turn to the KG-82s.
(e) PARITY lights (two):

1. GREEN light - indicates successful transfer and storage of keys with good parity.
2. RED light - indicates incomplete transfer or transfer with parity failure.

(f) DPE red indicator - indicates detection of a parity error during data transfer from the CS or MS which is reported to the HGX-84.
(g) POWER green indicator.
(h) FILL connector.
(i) BATTERY compartment.

NOTE: Show Slide 9. Refer to TM 11-5810-330-13.

f. Loop key generator (LKG), TSEC/KG-82-CCI.

(1) Operates when used with a HGX-82.
(2) Provides path for verification and electronic transfer of keys stored in the HUS.

(a) Provides synchronization and maintains secure passing of traffic between compatible COMSEC equipment.

(b) Uses a number of in-band and out-of-band signals.

(3) MS KG-82 operations.

(a) Dedicated to MS ports.
(b) Provides encryption interface for CS-to-MS trunks, MS-to-MS trunks, and MS data terminals.
(c) Can operate in three modes which can be selected by the use of the FUNCTION switch.

1. Mode 1 - CS to MS trunk.
2. Mode 2 - data terminals (loops) and trunks, redundant synchronization.
3. Mode 3 - data terminals (loops) and trunks, nonredundant synchronization.

(d) During initialization of KG-82s the operator must connect a fill device to the associated HGX-82 to transfer operating keys to the dedicated KG-82s. If a rekey operation is required for a terminal, the KG-82s can obtain a new key from the HUS using CMD 25 under operator control. This is using the RCU feature of the HGX-83.

(4) Controls and indicators - explain, using TM 11-5810-330-13, para 2-2.

QUESTIONS: The KG-82 is compatible with what other COMSEC devices? (ANS: DSVTs, KG-84s, and other KG-82s.)

KG-82s are dedicated to subscribers in what applications? (ANS: Message switch.)

NOTE: Show Slide 10. Refer to TM 11-5810-361-18, FM 24-27A, and KAO-l93A/TSEC. Inform the students that they may see KG-81s (older version) or KG-194 (newer version) instead of KG-94s in some publications and in field applications.

g. Trunk encryption device (TED), KG-94 - CCI.

(1) Purpose and use.

(a) The TED is a bulk encryption device which has the capability to encrypt up to 300 trunks simultaneously, over a single DTG.
(b) It is an on-line key generator which performs digital data encryption/ decryption in full duplex synchronous operation.
(c) Generates random patterns of ones and zeros which simulate a full traffic load at all times. This prevents unauthorized persons from being able to detect periods of peak traffic.
(d) Provides end-to-end bulk encryption of DTG traffic between:

1. MS-to-MS.
2. MS-to-CS.

(e) One trunk encryption device (TED), at a minimum, is used at each end of the secure DTG link. It may be located in either the switch or terminating radio van.

1. If multiple TED encryption/ decryption is utilized in a path, each set of TEDs will share a key that is unique to that pair of TEDs.
2. This use of "paired keys" is the source of the term pair-wise unique keys.

(f) The TED also has the ability to create permutations of its original key which are used at specified intervals to change the current traffic key to prevent detection or compromise of the originally loaded key. The original key loaded into the TED is known as the seed or cold start key and is also referred to as a TED traffic encryption key (T-TEK).

(2) Specifications.

(a) Passes traffic at a rate of 9.6 kilobits to 13 megabits per second.
(b) Designed for use in and around mobile, and sheltered environments.
(c) Can use a KYX-l3, KYX-l5/lA, or KOI-l8 to load keys.
(d) Operates on 19 to 56 VDC.
(e) Can be operated by controls on front panel or can be remotely controlled.
(f) Contains a battery and fuse to allow the storage of current traffic key and protection (TEK1 in case of power loss or serge).
(g) When the TED is removed from the mounting frame, the traffic key is automatically zeroized.

(3) Controls and indicators - explain, using TM 11-5810-361-10, para 2-1.

NOTE: Describe the basic use of the various controls/indicators.

(a) Indicators.

1. PARITY - Green LED lights to indicate that a valid key has been loaded.
2. OLD KEY - yellow LED lights to indicate an unsuccessful key change was attempted.
3. RESYNC - Green LED lights to indicate that synchronization between the local and remote (distant end) unit has occurred.
4. FULL OPR - yellow LED lights to indicate that the equipment is operational.
5. ALARM - red LED lights to indicate an alarm condition and informs operator that the KG-84 is no longer sending traffic.
6. PWR ON - Green LED lights to indicate that input power has been applied and that the logic and battery voltages are present.
7. UPDATE - a two-digit LED display shows the current count of the updated key.

(b) Controls.

1. ACTUATE - pushbutton switch used to initiate the test or operation selected by the FUNCTION switch.
2. FUNCTION switches -

   a. RESTART - begins synchronization in the current key after a power transient, crypto alarm, or unsuccessful change key.
   b. CHNG KEY - starts synchronization in a new key. If the KG is in FULL OPERATE, without adding a new key, the current key will be updated in both local and remote units.
   c. LOAD - transfers a key from a fill device to a storage location in the KG.
   d. LCL UPDATE - initiates update. The seed key (original traffic key) is updated at one end of the link, and a restart is initiated.
   e. ALARM TEST - start an alarm check sequence. It will not affect operation.
   f. LAMP TEST - lights all LEDs on the front panel.

3. POWER switches -

   a. ON - supplies power to the KG unit. Activates battery for key retention if power is lost.
   b. STBY- removes power, but retains key.
   c. OFF (ZEROIZED OFF) - power is removed. Key will be lost. The switch must be pulled before it can be set to OFF.

(4) Operation. The operation and configuration of the TED will be

discussed in a later lesson which will cover:

(a) Patching (if required).
(b) Loading keys.
(c) Performing change variable operations.
(d) Replacing and updating procedures.

h. Common equipment facilities and trunk encryption modules (CEF/TEM).

(1) Provides housing for COMSEC equipment.
(2) Distributes cooling air for the various items in the modules.
(3) Provides electrical interface for the various equipment in the modules.

QUESTIONS: The KG-194 is a bulk encryption device, but what does it do that prevents unauthorized persons from detecting peak traffic periods? ANS: It continuously generates random patterns of ones and zeroes to simulate a full traffic load.)

Can a TED be remotely controlled? If yes, explain. (ANS: Yes, when performing change variable operation from the controlling end.)

NOTE: Show Slide 11. Refer to TM 11-5810-309-10 and KAO-l93A/TSEC (C).

j. Dedicated loop encryption device (DLED), KG-84A.

(1) Encrypts and decrypts teletypewriter or other communications terminal devices, both analog and digital, for data transmission through the TRI-TAC/MSE network. When used for analog equipment, some type of modem is required between the analog system path and the DLED.
(2) In TRI-TAC operations, the KG-84A is utilized in the full duplex mode.
(3) Contains the necessary electronics for:

(a) Storage, processing, and control.
(b) Clock.

(c) Data recovery.

(4) Storage battery to retain keys when the DLED is powered off.
(5) In MS operation, communication terminals such as the AN/UGC-74 or AN/UGC-l44 are dedicated to MS ports. KG-84As are then compatible with the KG-82s between an AN/TYC-39 dedicated LKG and an external DLED associated with the communication terminal. The external KG-84A may also serve as a diphase loop modem when used with a digital MS data subscriber.
(6) Remote MS terminals utilizing KG-84As can gain access to the MS via dedicated or dial-up paths through the CS.

NOTE: Show Slide 12.

(7) Controls and indicators - explain location and functions, using TM 11-5810-309-203, para 3-2.

(a) Operator controls - located on the lower half of the KG-84A front panel.
(b) Concealed controls - concealed behind the protective cover on the top half of the KG-84As front. They are normally set at initial operation according to the specific communications system or unit SOP.

QUESTION: What is the primary use of the KG-84 DLED? (ANS: Used to provide crypto services for MS terminal devices.)

NOTE: Show Slide 13. Refer to TM 11-5810-329-10 and KAO-l93A/TSEC (C).

k. TSEC/KY-68 digital subscriber voice terminal (DSVT). The KY-68 operates as a full duplex voice/data terminal for 16 or 32 kb/s traffic. The KY-68 provides the cryptographic functions, audio processing, and signaling necessary for secure and nonsecure access to switched networks, and secure point-to-point operation.

(1) Applications.

(a) Point-to-point - when loaded with the same keys, two KY-68s will function in a secure mode and the distant-end will ring as a result of the first phone going off-hook.

(b) Circuit switch interface - this is the normal interface and in this mode the KY-68 is connected to a KG-82 inside the circuit switch for initial synchronization and key verification. In circuit switch applications, the KY-68 can be operated in two basic modes:

1. MODE 1 - used exclusively with a COMSEC parent switch (AN/TTC-39s or AN/TTC-42), whereby the COMSEC network supplies a different "V" key for each call processed by the COMSEC parent switch.
2. MODE 2 - can be used with either a COMSEC parent switch or a COMSEC subordinate switch (5B-3885), and traffic can be passed with either a per call variable (V) or a network variable (X).

a. MODE 2 is also used for point-to-point operation, which is also called the sole user mode.
b. For greater flexibility, it is recommended that all KY-68s be strapped for MODE 2 operation.

(c) Extension.

1 An extension DSVT may be connected off of another DSVT, but there are limitations to the use and operation of the extension DSVT.

a An outgoing call cannot be dialed from the extension phone.

b There is no indication on the extension phone that a call is being initiated from the primary DSVT or that the primary DSVT is in use.

c The extension phone will not receive an audible ring on an incoming call; however, the ring/busy LED will blink in synchronization with the incoming ring signal and the non secure warning (NSW) LED will illuminate at the normal rate.

2 The DSVT is connected as a subscriber of the circuit switch (primary).

a Both DSVTs will be programmed alike, set for MODE 2 operation and loaded with the same keys.

NOTE: Show slide 14

b The extension DSVT is powered from the HYP-7l aux power supply.

c Special purpose cable must be fabricated to connect the two DSVTs. It should not exceed 100 feet in length, and must be fabricated using shielded cable.

3 The DSVT was not designed to be used as an extension phone. When connected as an extension, the primary DSVT must be used to initiate an outgoing call or answer an incoming call.

4 When connected to another DSVT, the extension DSVT can be used to meet the operational requirement for extending a DSVT call to a private office or to a less noisy location.

NOTE: Show slide 15.

(d) User controls, lights, and audible indications. The following controls, lights, and tones will be used or are present when receiving or placing calls:

1 Keyboard switch matrix.

a Three buttons labeled R, P, and C are used for special applications.

R - used in conjunction with the net radio interface (NRI).

O - used for operator recall.

C - used for initiating special switch functions such as conference and commercial access, and to release conferences or to indicate the end of a dialing sequence.

b In AN/TTC-39D and MSE applications, the keyboard is also used to affiliate and disaffiliate a subscriber.

2 Audio volume control. Used to adjust the audio level in a handset or headset.

3 Ring volume control. Used to adjust the ring and tone level in the annunciator (electrically controlled indicator).

4 Cradle hookswitch.

a When the handset is placed on the cradle or ON-HOOK,

b When the handset is removed from the cradle or OFF-HOOK.

c Pulling the hookswitch to its uppermost position establishes the plain text mode.

d When operating in the data mode, or when using a handset, the hookswitch can be pushed all the way down and rotated to the right to lock it in the ON-HOOK position.

5 Ring/busy light. When the KY-68 is being called in the voice mode, the red RING/BUSY light flashes at a rate of 1/2 second on and 1/2 second off.

6 Nonsecure warning (NSW) light. This red light supplements the nonsecure warning tone heard in the earpiece and indicates that an OFF-HOOK terminal is operating in a nonsecure mode.

a The DSVT assumes a nonsecure mode for all calls and provides nonsecure warning indicators and tones until it is signaled into secure traffic by the circuit switch.

b The light flashes (50 milliseconds ON once per second) when indicating a nonsecure call.

7 Ringback. This tone is present at a 2 second on, 4-second off rate to indicate ringing of the called party and is heard in the handset.

8 Ring. This tone is present at a 2-second on, 4-second off rate to

indicate an incoming call and is heard via the annunciator.

9 Digit sidetone. This tone is present as long as any keyboard digit is pressed during the dial phase or affiliation process.

10 Nonsecure warning. When locally generated, this tone is present (50 milliseconds ON) once every 6 seconds. When inserted in the middle of the 4-second ringback tone for ease of detection.

11 Crypto alarm, This is a continuous tone and alerts the user that a crypto alarm condition exists. The secure operation of the KY-68 is disabled during a crypto alarm condition,

(e) Initialization controls and indicators.

The following controls and indicators will be used during the initialization (loading keys) of the DSVT:

1 FUNCTION SELECT switch:

a SVAR - used for loading the S key, permits S mode operation.
b OP - puts the DSVT in normal operation when initialization is complete.
c LDX - used for loading the X or NET key.
d LDU - used for loading the U or unique key.
e DSBL - disable all local operation of the DSVT, extensions, and data devices. Sends MASTER RESET command to internal circuits.

2 VAR STOR switch - works with the FUNCTION SELECT switch.

a Center position - normal operations.
b LOAD position - allows key loading.

c ZERO position - zeroizes all stored keys.

QUESTIONS: What mode is recommended that the KY-68s be left set to? (ANS: MODE 2 for greater flexibility.)

What are the four hookswitch positions and what do they do? (ANS: ON-HOOK, OFF-HOOK, plaintext mode, and ON-HOOK and LOCKED for data mode or when using a headset,)

What indications does the KY-68 provide to inform the user that they are connected to a nonsecure party? (ANS: Nonsecure warning light and nonsecure warning tone once every 6 seconds.)

2H 55M

4. Practical exercise.

NOTES: This practical exercise involves the students answering questions concerning the functions of the various pieces of COMSEC equipment, therefore, when ANY entries have been made, the entire PE becomes classified CONFIDENTIAL. DO NOT leave these PEs unattended after issuing them to the students. Collect them after class and instruct the students that they may have them back for study purposes but they MUST be returned to the instructor after each class session.

Explanation to students.

(1) This practical exercise provides you the opportunity to recall the functions of COMSEC equipment utilized in both CS and MS applications. An understanding of this equipment will be of immense value to you in your daily duties as a 74G operating and maintaining the TRI-TAC switches in a network. Within a time limit of 1 hour, you must correctly answer 14 of 20 questions.

(2) This practical exercise is not classified until ANY question(s) have been answered. The document is then classified CONFIDENTIAL. After you have answered any questions, DO NOT leave the practical exercise unattended.

b. Application by students.

(1) Enter the common name of the piece of equipment listed and a brief short answer description of its purpose.

(2) For questions 18 - 20, provide the information requested.

(3) Ask your instructor for assistance if required.

(4) Have your instructor check your work when completed.

c. Evaluation.

During the practical exercise, evaluate the ability of each student to meet the prescribed objective within the standards set in the lesson.

3H 55M

SUMMARY:

During the lesson, we have discussed the functions and applications of the many pieces of COMSEC equipment that you will be required to use as part of your everyday routine in TRI-TAC switches. One of the greatest assets of a TRI-TAC switch is its ability to provide COMSEC services for its subscribers and the network. Without COMSEC, these switches become virtually useless.

4H

END

This document supports Task Number 113-603-3205.

U.S. ARMY SIGNAL CENTER AND FORT GORDON
Fort Gordon, Georgia 30905-5180

LESSON PLAN

TITLE: Key/Variable Functions

LEARNING OBJECTIVE:

Action: The student will receive instruction relating to the functions of the various COMSEC keys used in TRI-TAC systems.

Conditions: The student is given TMs 11-5805-778-12-1 through 11-5805-778-12-7, classified publications FM 24-27A (C), and Information Sheet 3, 150-74G10/C01-LP3-IS-3.

Standards: The student will answer verbal questions during the conference when called upon by the instructor.

SAFETY CONSIDERATIONS: There are no safety considerations for this lesson.

RISK ASSESSMENT: Low.

RESOURCE NEEDS/ REFERENCES: TMs 11-5805-778-12-1 through TM 11-5805-778-12-7 and classified publications FM 24-27A and KA0-193A, overhead projector, slides 1-2, TB 380-40, JCS Pub 6-05.5, and TM 11-5810 Series of manuals.

METHOD OF INSTRUCTION: Conference

TIME: 2 Hour 30 Minutes

APPROVAL DATE: 24 NOV 97
DEVELOPER: SFC CARTAGENA
DIV. CHIEF: Jack P. Rondon

NOTES TO INSTRUCTOR:

1. Ensure the publications listed in the conditions statement are available to the students.

2. Obtain the necessary slides or handouts if applicable.

3. Ensure that the students are issued their communications security (COMSEC) notebooks for the lesson and secured during breaks or picked up and secured at the end of the day.

4. Ensure that the doors to the classroom are closed and no unauthorized persons are present during the conference.

INTRODUCTION:

Elapsed Time

1. In previous lessons, you became familiar with the fundamentals of COMSEC and the various COMSEC devices utilized in the TRI-TAC environment.

2. Key variable functions apply to all TRI-TAC COMSEC that is used by personnel involved in planning, installing and managing record data and special purpose communication systems which are used to support joint exercises and contingency operations.

3. During this lesson, we will discuss the many COMSEC keys that are utilized in this equipment. The focus of this lesson is to familiarize yourself with the different types of keys and their specific uses.

5M

BODY:

1. Importance of key.

   a. The key and the cryptographic logic, which is built into COMSEC equipment, encrypts the information being transmitted. The logic is fixed within the equipment; only the key can be changed. This makes the key crucial to the secure operation of a cryptonet.

b. If both the key and logic remain unchanged for a long enough period, sufficient traffic can be passed to provide intelligence analysts enough material to "break the code".

c. The key, therefore, must be changed frequently to reduce the impact of a compromise and the likelihood of successful cryptanalysis.

d. How frequently keys are changed depends upon the size of the cryptonet and amount of traffic passed over it.

QUESTION: Why is it vital that the key be changed periodically? (ANS: Because the logic is fixed and changing the key prevents the enemy from breaking the code.)

10M

2. Physical forms of keys.

a. Keys exist in the TRI-TAC COMSEC equipment as a series of randomly generated electronic bit streams consisting of 128-bits per key.

b. Originated by two different methods:

(1) National Security Agency (NSA) generates and punches keys onto paper tape, then packages and distributes the keys to users as required.

(a) These tapes, commonly called hard copy keys, have an advantage because they can be stored for long periods before use.
(b) They are not vulnerable to electronic interference such as electromagnetic pulse (EMP).
(c) May be pre-positioned worldwide using existing courier systems.
(d) Disadvantages include:

1. Expense to produce and distribute.

2. Lengthy ordering and shipping time.
3. Detailed accounting required.
4. Vulnerable to compromise while in transit and storage.

(2) Generated electronically by a certified key generator such as the KG-83 and distributed, as needed, using a fill device such as the KYX-l3 or KYK.

(a) Basic rules allow some keys to be transmitted electronically to users.
(b) Advantage is that they have reduced vulnerability because they are not stored for long periods prior to use.
(c) Disadvantages include:

1. Less strict accounting creates difficulty in knowing who has certain keys in case of compromise or enemy overrun situations.
2. Electronic transfer of certain keys may not be permitted.
3. Because keys cannot be labeled as on a tape, the possibility of confusing them with other keys is increased.

(3) Overall, for most tactical employment, the advantages of electronically generated keys outweighs those of hard copy keys.
(4) Locally generated electronic keys will be the primary key source for TRI-TAC networks.
(5) Hard copy keys will continue to be required for contingency keys to recover from EMP and for certain operations in which keys need to be held for long periods by geographically separated forces.

QUESTIONS: The electronic key (bit stream) consists of how many bits? (ANS: 128.)

What will be the primary source of key for TRI-TAC networks, hard copy or electronically generated? (ANS: Electronically generated.)

20M

3. Types of keys.

NOTE: In the past, the term variable was used extensively. The use of the term variable is being replaced with the term KEY. Many NSA and Army publications contain or continue to use the old terminology. Existing COMSEC equipment has the term VARIABLE or VAR printed on them. To end the confusion and reduce the number to terms, two variations of key will be used, traffic encryption key (TEK) and key encryption key (KEK).

a. TEK.

(1) Used to protect (encrypt) operational traffic (voice, data, video) from unauthorized disclosure or manipulation and as synchronization signals.
(2) TEKs are classified at the highest level of the traffic they will encrypt.
(3) TEKs are further divided into subcategories that describe their specific use.

(a) T TEK - Trunk encryption device (TED) key used for digital transmission groups inconjunction with a TED to encrypt an entire transmission path.

1. Used at each end of a transmission path.
2. Unique to each pair of TEDs, also known as a SEED key.
3. Must be updated daily, usually during low traffic periods.

4. Used in both circuit switch (CS) and message switch (MS) applications.

(b) X TEK - traffic key:

1. For the AN/TYC-39 MS, the “X” key is used to encrypt/decrypt traffic on a KG-82 to KG-84 loop.
2. Each loop will have a different X-traffic key.
3. The “X” traffic key will also be used on trunks between AN/TYC-39 MS (LKG-to-LKG).
4. An initial synchronization key (X-SYNC key) can only be used to initialize KG-84s and dedicated KG-82s. The X-SYNC variable must be replaced with an X-traffic key before passing traffic.

NOTE: Selected subscribers use the TSEC/KY-68 digital subscriber voice terminal (DSVT) to connect to the CS. These subscribers are encrypted on an end-to-end basis with the “V” key and “S” key for high security.

(c) V TEK - per call key:

1. The key is uniquely generated by the COMSEC PARENT SWITCH (CPS) to encrypt/decrypt a DSVT subscriber’s conversation.
2. A new key is generated for each call.

(d) S TEK - special HIGH classification key:

1. This key is held only by subscribers and not at switches.
2. Used by small select communities for discussing TOP SECRET over DSVTs.
3. It can only be distributed by courier, either in hard copy key

material or in an electronic keying device.

b. KEK.

Used to encrypt another key so it may be transmitted electronically or stored securely.

(a) KEKs will not be used to encrypt traffic or signalling information.
(b) Normally generated electronically and stored in the automatic key distribution center (AKDC) or a fill device.
(c) Also held in electronic form in various COMSEC devices, such as the KY-68 or the KG-84, where it is used.
(d) May originate in hard copy paper tape if required.
(e) A KEK is classified at the highest level of TEK it will encrypt.
(f) Physically distributed by courier, not permitted to be electronically transferred.
(g) KEKs are further divided into subcategories that describe their specific use:

1. Z KEK - Used to encrypt all keys stored in the hardened unique storage (HUS) of the AKDC.

a. As a key is transferred into or out of the HUS it is encrypted/decrypted with the storage Z KEK.
b. In the event of an emergency or overrun situation, the storage “Z” may be zeroized and the contents of the HUS rendered useless.

c. If authorized control of the AKDC is re-established; access to the stored keys can be regained by reinserting the storage Z KEK.

40M

d. Z KEKs are unique to each MS or CS and are generated electronically in the switch as needed.

e. May not be transmitted electronically.

f. Should be kept as a fill device in the event that the AKDC required is changing due to failure or it is zeroized for any reason.

g. Must be stored in a secure location other than the switch where it is used, generally in a safe in the maintenance or prescribed load list (PLL) shelter.

2. U KEK - the rekeying key:

a. Used to secure electrical transmission of other cryptovariables between the MS and KG-84s or between two MS to AUTODIN interfaces.

b. The U KEK is distributed by courier and it is wise for the terminal operator to maintain it in the event that the KG-84A is changed or zeroized.

c. The MS maintains the Us in the AKDCs HUS or a fill device.

c. Contingency keys.

(1) On a large complex and rapidly moving battlefield, there exists the possibility that large portions of a network may loose electronic keys.

(2) This could be because of several factors:

(a) Zeroized equipment in anticipation of an overrun.
(b) Actual overrun.
(c) Compromise.
(d) Result of an EMP event.

(3) Contingency keys are pre-positioned throughout the network before they are actually needed.
(4) Generally stored on paper tape since it is not vulnerable to EMP or other electrical upset.
(5) An additional type of contingency key is held only by COMSEC custodians of units who may have requirements to transfer TEKs between each other using DSVTs and KYX-l5As. The key must be destroyed within 24 hours of first use.

QUESTIONS: Of the several versions of keys, what are the two primary types of keys? (ANS: TEK and KEK.)

In addition to the two primary key types, there is a third key, that supplements the primaries, what is it? (ANS: Contingency key.)

What is the Z KEK used for? (ANS: To encrypt all keys in the HUS.)

What is the V TEK used for? (ANS: Per call encryption key.)

Explain why it is so important to have contingency keys? (ANS: To zeroize equipment in anticipation of an overrun, actual overrun, compromise and or result of an EMP event.)

50M

4. Application and use of keys.

a. As previously mentioned, it is the responsibility of the system planner and the key variable management planner to develop both the network configuration and assignments of switch IDs needed for bulk transfer and decide which switch is responsible for key generation.

b. Source of keys - as we discussed earlier, the primary source of keys will be local generation; however, others may come from either:

(1) Brigade - provided by COMSEC custodian prior to deployment.
(2) IC^3S - Intertheater command, control, communications (C^3) security will generally provide paper tape keys used for contingencies or widely separated units.

c. Brigade key/variable manager - assigns the following:

(1) Area codes to be used in the network using MYX format.
(2) All 39D and node center switch (NCS) codes using XX format.
(3) All LEN switch codes in the LXX format.
(4) All 39A and other required switch codes in the NNXX format.

1H

5. Management of keys.

a. Background.

(1) Extensive systems such as TRI-TAC with large numbers of keys have created the need for automated planning, accounting, distribution, and identification of keys.
(2) There are plans to add a formatted key "tag" to the normal 128-bit key.

(a) The key "tag" would contain designated fields to correlate it to a specific COMSEC system; type of equipment; cryptoperiod; classification; and so forth.
(b) Other information useful for identification, control and accounting, and free format text may be entered by the user.

(3) Until such time as these devices are distributed to all COMSEC systems, the management of keys using a manual system is necessary for the following reasons:

(a) Orderly generation and/or distribution of new key.
(b) Normal supersession at the end of a crypto period.
(c) Emergency supersession of compromised keys.
(d) Assure that the correct key is distributed to the right equipment for the right use.

(4) Key Management (KM) plan.

(a) The primary purpose of the KM plan is the accurate distribution of keys around the battlefield.
(b) As much as possible, electronic distribution using Over-the-Air-Rekey (OTAR) is preferred.

1. Only TEKs may be transferred using OTAR by subscribers.
2. TRI-TAC switches and COMSEC custodians for instance, a variation of OTAR, Manual Cooperative Key Transfer is preferred as it provides for a more secure method of key transfer than OTARs via a KY-57.

a. A TRI-TAC switch may transfer the U KEK only when encrypted by the interswitch key encryption key (IKEK).
b. The COMSEC custodian may transfer the U KEK only when encrypted by the COMSEC custodians' key encryption key (CCKEK).

b. Controlling authorities. In the TRI-TAC arena, there are two basic levels that are responsible for the management of keys.

(1) The Controlling Authority (CONAUTH).

(a) The commander of the organization performing the overall network planning and design is the CONAUTH, usually the brigade to which the TRI-TAC switches are assigned.
(b) The CONAUTH has the following responsibilities:

1. Designates Cryptonet Control Stations (CNCS) for every key generated or key tape used.
2. Designates the classification levels of all keys generated.
3. Outlines the distribution of keys to include contingency rekeying plans.
4. Monitors the key status and cryptonet operations.
5. Reports COMSEC insecurities and evaluates insecurities.

(2) CNCS.

(a) The CNCS is the control terminal for each trunk/circuit. In many circumstances, the AN/TTC-39s perform the functions of the CNCS.

(b) Once the network is designed, each CNCS is responsible for generating, storing and distributing all keys for which it has been designated the cryptonet controller.
(c) The CNCS is also responsible for the proper COMSEC operation of its network to include reporting COMSEC insecurities.

(3) KM plan.

(a) To determine key requirements and administrative control of key generation and distribution, both the CONAUTH and CNCS must prepare KM plans that cover their areas of responsibility.
(b) In developing the TRI-TAC each CNCS and also specify which keys each CNCS will generate. CONAUTH KM Worksheet (DA Form 5251-R) is used for this purpose.

NOTE: Show Slide 1.

(c) The CNCS will use the information on DA Form 5251-R to aid in control of key generation, distribution and use within its portion of the network. Management and control of all keys within the CNCSs area of responsibility are accomplished utilizing the CNCS KM Worksheet (DA Form 5251-1-R).

NOTE: Show Slide 2.

(d) These worksheets will become classified when data is entered with a level determined by the COMSEC custodian.
(e) When storing keys in a fill device, each key must be labeled with the key "tag" or ID which is recorded on the KM worksheets, not an "operator simple" label such as (site) "O2 T" (key).

(f) By following this procedure, a lost fill device will be of little value to the enemy without the appropriate KM worksheet (which is kept locked in a safe) to identify which key is used for a specific purpose.

(g) Any key stored in a fill device must be labeled correctly, if not, the holder of that fill device has committed a COMSEC insecurity and is subject to punitive action.

QUESTIONS: What is the preferred method of transferring electronic key? (ANS: OTAR, or Manual Cooperative Key Transfer at switch level.)

Where should the KM worksheets be kept when not actually being used? (ANS: In the safe to prevent unauthorized access or disclosure.)

2H 25M

SUMMARY:

During this lesson, we discussed the major keys used within the TRI-TAC network and their purpose. The importance of keys to the operation of the 39 family of switches cannot be overemphasized. Without proper utilization of COMSEC, the AN/TYC-39A is virtually useless. The information presented here is intended to be a base which you can build your first assignment with a 39 switch.

2H 30M

END

This document supports Task Number 113-603-3219.

U.S. ARMY SIGNAL CENTER AND FORT GORDON
Fort Gordon, Georgia 30905-5180

LESSON PLAN

TITLE: Communications Security (COMSEC) Initialization

LEARNING OBJECTIVE:

Action: The student will perform cold start initialization of the COMSEC subsystem.

Conditions: The student will be provided with an operational AN/TYC-39A with fully populated HGF-83 common equipment facility, TM 11 5810-256-OP-5, TM 11-5810-309-10, TM 11-5810-323-12, TM 11-5810-326-13, TM 11-5810-327-10, TM 11-5810-329-10, TM 11-5810-330-13, TM 11-5810-331-13, TM 11-5810-336-10, KAO-193A (C), fill device(s) with cable(s), and the practical exercise.

Standard: Acceptable performance is achieved when the student can correctly perform cold start initialization of the TRI-TAC COMSEC subsystem within 45 minutes.

SAFETY CONSIDERATIONS: There are no safety considerations for this lesson.

RISK ASSESSMENT: Low.

RESOURCE NEEDS/ REFERENCES: AN/TYC-39A with fully populated HGF-83 common equipment facility, TM 11 5810-256-OP-5, TM 11-5810-309-10, TM 11-5810-323-12, TM 11-5810-326-13, TM 11-5810-327-10, TM 11-5810-329-10, TM 11-5810-330-13, TM 11-5810-331-13, TM 11-5810-336-10, KAO-193A (C), fill device(s) with cable(s), practical exercise, slides 1-2, and overhead projector.

APPROVAL DATE: 24 NOV 97
DEVELOPER: SFC CARTAGENA
DIV. CHIEF: Jack P. Rondon

METHODS OF
INSTRUCTION: Conference, Demonstration, Practical Exercise.

TIME: 8.5 Hours

NOTES TO INSTRUCTOR:

1. Ensure all required TMs are available prior to class.

2. Ensure the students observe proper safety precautions.

3. Ensure that all necessary patch cords/looping plugs are on hand.

4. Ensure that fill devices with cables are available.

5. Maintain class roster for all COMSEC materials required by students during this class.

INTRODUCTION:

1. In previous classes, you became familiar with the functions of the various COMSEC devices that are utilized within the TRI-TAC family of switches, which are housed within the several common equipment facilities mounted within the various TRI-TAC switches. You also had a look at the combination of keys that these devices use.

2. Next, we will identify the various common equipment facilities that you will encounter within the TRI-TAC family of switches. We will provide you with the knowledge needed in order to initialize the COMSEC subsystem that is mounted within the HGF-83 common equipment facility C1-7.

3. This process may seem confusing or difficult at first, but once you master it, it will become second nature to you. The 39 family of switches MUST have their COMSEC working, so pay attention and you should have no difficulty.

3M

NOTE: Explain to students the COMSEC regulations as outlined in Information Security Program. Regulation DOD 5200.5 1-R and TRADOC Pam 525-40 must be observed at all times.

BODY:

1. Initialization requirements.

   a. The term "initialization" refers to all actions taken to set-up, turn-on, and operate the message switch (MS) AN/TYC-39A when it enters service in a deployed joint task force (JTF) network.

   b. The following steps summarize MS initialization:

      (1) Cabling and connections.
      (2) Power-on procedures.
      (3) Message processor start-up.
      (4) Setting variable parameters.
      (5) Data entry.

   c. COMSEC initialization.

      When initialization actions are complete, you must initialize the required COMSEC equipment. To do this you must refer to Standing Operation Procedure (SOP), Operation Order, and Planning Worksheets to find which circuits need keys, which use hard copy keys (cards, tape), or which require electronic keys.

   d. COMSEC procedure:

      (1) Start by "initializing" the HGX-83/ telecommunications security (TSEC) automatic key distribution center/ rekeying control unit and load your electronic keys into it.
      (2) Use the key variable generator TSEC/KG-83 to generate the electronic keys for which you are responsible.

(3) If you do not have an HGX-83/TSEC available, you should load the electronic keys into the electronic fill device KYK-13 or KYX-15 provided. Then, load keys into the loop key generators (LKG) that you require.
(4) Next, you load electronic keys into the trunk encryption devices (TEDs) assigned to the active transmission groups.
(5) When this is completed, you make a written record of key locations in the HGX-83/TSEC fill device, the LKGs assigned, and note all of the other decisions that have been made.

QUESTION: What does the term " initialization" mean? (ANS: The term "initialization" refers to all actions required to set-up, turn-on, and operate your equipment in a JTF network.)

10M

NOTE: Show Slide 1.

2. Common equipment facilities.

a. Purpose and use.

The common equipment facility is used to provide ruggedized housing for equipment used in COMSEC modules CI-5, CI-7, and CI-8. These assemblies are designed to provide the following:

(a) Housing for COMSEC modules CI-5 (HGF-82), CI-7 (HGF-83) and CI-8 (HGF-85).
(b) Distribute cooling air for the various COMSEC equipment used in the COMSEC modules.
(c) Electrical interface for the various COMSEC equipment used in the COMSEC modules.

The common equipment facility HGF-82 (CI-7), HGF-83 (CI-8), and HGF-85 (CI-8) are all three used to provide TRI-TAC

COMSEC in the 39 family of automatic switches.

b. The MS AN/TYC-39A utilizes the HGF-83 (CI-7) and it houses the following equipment:

(1) Two HGX-84.
(2) Two KG-83.
(3) One HGX-83.
(4) Forty-eight KG-82.
(5) Six HGX-82s.
(6) Three KG-81 (KG-94).

QUESTION: What is the maximum number of HGX-82/TSEC that is used within the HGF-83 (CI-7) ruggedized equipment rack? (ANS: The TSEC/CI-7 equipment rack will hold a maximum six HGX-82/TSECs.)

15M

3. COMSEC initialization of the COMSEC subsystem.

a. Purpose.

The purpose behind getting the equipment up and functional first should be obvious. The HGX-83/TSEC is where all of the keys are maintained for later use in the system and externally by the subscribers.

b. Cold start procedures.

(1) Your first step is to ensure that the COMSEC fan circuit breakers, COMSEC 1 and COMSEC 2, located on the power distribution panel are ON.
(2) Now, let's check to ensure that the circuit breakers at the top of the HGF-83 rack are in the ON position.

NOTE: Explain that the fan (center) circuit breaker must be set to ON prior to the HGX-84 circuit breakers (failure to do this causes them to stay tripped).

(3) Next, let's energize (power on) both HGX-84/TSECs. Put both HGX-84s on-line.
(4) Next, we energize both TSEC/KG-83s. Initialize both KG-83s IAW TM 11-5810-331-13.
(5) Then, we energize (power on) all HGX-82/TSECs. Initialize each HGX-82 IAW TM 11-5810-326-13.
(6) Next, let's power up and initialize each required KG-82/TSEC IAW TM 11-5810-326-13, para 2-7, for the MS with the key being loaded (obtain the key from the TSEC/KG-83).

NOTE: Explain to the students that the start-up procedure of the HGX-83/TSEC consist of powering up and loading the Z-variable on a newly installed unit, or a unit that has been zeroized.

(7) Start-up procedure for the automatic key distribution center rekeying control unit HGX-83/TSEC IAW TM 11-5810-327-10, para 2-4 through 2-6.

QUESTION: Why must the fan (center) circuit breaker be set to ON, prior to the HGX-84s being turned on? (ANS: Failure to set the fan (center) circuit breaker on before HGX-84s are turned on will cause the circuit breakers to stay tripped).

45M

NOTE: Show Slide 2.

4. Load procedures.

NOTE: Explain to students that when the HGX-83/TSEC is used with the AN/TTC-39A/D (PS) circuit switch, one HGX-83/TSEC operates on-line and the other operates off-line as determined by the switch.

a. Command "59" (Clear Error).

NOTE: Refer students to TM 11-5810-327-10, para 2-7, pg 2-22.

(1) With an on-line HGX-83/TSEC you dial in the right command to clear error.
(2) If an unallowable command or address is tried, error light will come on - display will show "00".
(3) Dial clear on function switch if off-line. Then push and release start button.

b. Command "91".

Command "91" changes the Z-variable in a stand-alone HGX-83/TSEC.

NOTE: Refer students to TM 11-5810-327-10, para 2-7 for further information.

(a) Operate POWER switch on.
(b) Set MANUAL mode COMMAND/ADDRESS switch to "0091" by using the thumbwheels.

NOTE: Explain that this must be done off-line.

(c) Set MANUAL mode FUNCTION switch to "CMD".
(d) Push and release the START button.
(e) CMD No light comes ON.
(f) "91" is be displayed.
(g) Open access door.

NOTE: Explain that opening access door will cause crypto and Z-zero alarms to light and major alarms to energize.

(h) Crypto and Z-zero alarm indicators will stay on.
(i) Zeroize indicator blinks, then goes off.
(j) Connect selected fill device either KYK-13 or KYX-15A to the HHX-83/ TSEC IAW TM 11-5810-327-10, para 2-7, pg 2-26 and pg 2-2-27.

1. Press and release Z-fill button.
2. PARITY indicator on fill device lights.

3. Close and latch Z-fill door, with firm even pressure.
4. HUS ON will light and stay on for 20 seconds.
5. Z-Zero alarm light goes out as soon as door closes.
6. CMD No and display blank after 20 seconds.

(k) Your Z-variable is now ready for use.

NOTE: Explain to students that if the crypto and Z-Zero alarms stay lit, the loading procedures must be repeated - If they are on after second attempt, check fill device.

1H 10M

c. Command "57".

NOTE: Refer students to TM 11-5810-327, para 2-7, pgs 2-55 through 2-61. Command "57" is used to load variable from "HUS". Explain that command "57" can be performed with either KYK-13 or KYX-15/15A, and although the procedures are not identical they are similar.

(1) On the KYK-13, set FILL switch to desired location.
(2) Set MODE SELECT switch to "Z".
(3) Press and release INITIATE button.
(4) Turn MODE SELECT switch to OFF/CHECK.

NOTE: Explain that this zeroizes the KYK-13.

(5) Turn MODE SELECT switch to ON.

NOTE: Explain to students that you must be certain ADDRESS SELECT switch is set to correct location.

(6) Insert connector J1 into fill connector of HGX-83/TSEC and turn to lock.
(7) At COMMAND/ADDRESS thumbwheels, dial in "0057".

(8) Set FUNCTION switch to "CMD".
(9) Press and release START button.
(10) CMD No and ADRS A lights come on.
(11) Display will show "57".
(12) Dial in the number for the variable.
(13) Turn FUNCTION switch to ADRS "A".

NOTE: Explain to students that after the next procedure, they MUST initiate within 7 seconds.

(14) Press and release START button.
(15) CMD No stays On.
(16) Display stays "57".
(17) ADRS A light goes out.
(18) HUS ON will blink on off-line HGX-83/TSEC - within 7 seconds.
(19) Press and release INITIATE button.
(20) PARITY indicator will blink.
(21) CMD No light goes out.
(22) Display goes blank.
(23) Turn KYK-13 MODE SELECT switch to OFF/CHECK.
(24) Disconnect KYK-13 from HGX-83/TSEC.

NOTE: Explain to students that the procedures for loading with a KYX-15/15A are similar. Refer students to TM 11-5810-327-10, para 2-7, pgs 2-62 through 2-67.

1H 30M

d. Command "75".

NOTES: Refer students to TM 11-5810-327-10, para 2-7, pgs 2-70 through 2-78. Command "75" is used to load "HUS" from fill device.

Explain to students that Command "75" can be performed with either KYK-13 or KYX-15/15A, and although the procedures are not identical, they are similar.

(1) Connect the KYK-13 electronic transfer device to the HGX-83 by the fill cable.
(2) Set KYK-13 MODE SELECT switch ON.

NOTE: Explain to students that ADDRESS SELECT switch MUST be set to correct location.

(3) At COMMAND/ADDRESS thumbwheels dial in "0075" by using thumbwheels.
(4) Set FUNCTION switch to "CMD".
(5) Press and release START button.
(6) CMD No and ADRS A lights come on.
(7) Display shows "75".
(8) HUS on light will come on.
(9) Dial in the desired HUS number.
(10) Set FUNCTION switch to ADRS A.
(11) Press and release START button.
(12) CMD No and ADRS A lights go out.
(13) Display goes blank.
(14) HUS on light will come on.
(15) HUS light will come on both HGX-83s if used.

NOTE: Explain that if the error light does come on, Command "75" was not completed. If you are using an off-line HGX-83, perform a command "89". This will tell you if you should repeat command "75" or, if your HGX-83 needs maintenance.

(16) If command "75" was completed, set KYK-13 MODE SELECT switch to OFF/CHECK.
(17) Disconnect KYK-13 from HGX-83.

e. Command "89".

Command "89" is used to check about 70 percent of the HGX-83 logic, it also checks battery voltage.

NOTE: Explain that this command must be performed off-line.

(a) Ensure that the associated KG-83 alarm light is not on.
(b) Be sure that the HGX-83 on-line light is not lit.
(c) At the COMMAND/ADDRESS thumbwheels dial in "0089" by using thumbwheels.
(d) Set FUNCTION switch to CMD.

(e) Press and release START button.
(f) CMD No light comes on.
(g) Display shows "89" then goes blank.
(h) If error light comes on, display will show area where the error occurs.

NOTE: Explain that in the event that the HGX-83 requires maintenance, it must be shipped to the limited maintenance personnel.

(10) If the BTY LOW light comes on, change battery and repeat command "89".

QUESTION: Why is it a good idea to initialize the HGF-83 (CI-7) common equipment facility, prior to the other COMSEC within the switch? (ANS: The CEF contains the HGX-83/TSEC which is the storage location for all the keys to be used by the switch and its subscribers.)

lH 50M

NOTE: Reshow Slide 1.

5. Trunk Encryption Module (TEM).

a. The TEM contains, as you know, additional TEDs to provide encryption for DTGs.

b. The initialization procedure for the TEM is quite simple consisting of the following steps:

(1) Check to ensure that the TEMl and TEM2 circuit breakers were previously turned ON at the power distribution panel.
(2) Place the FAN (center) circuit breaker ON. (Failure to set this breaker ON prior to the HGX-84 breakers causes them to stay tripped.)
(3) Place HGX-84 unit 1 (left) circuit breaker ON.
(4) Place HGX-84 unit 2 (right) circuit breaker ON.
(5) Individual TED initialization will be performed in a later lesson.
(6) Place the POWER switch to the STBY position on all populated TEDs. (This

prevents them from reporting a false status to the processor which may induce alarms.)

2H

6. Demonstration.

a. Divide the class into groups and rotate them through the switch during demonstration.

b. Use the practical exercise as a guideline to demonstrate the cold-start initialization of the COMSEC subsystem.

2H 30M

7. Practical exercise.

a. Explanation to students.

(1) During this practical exercise, you will perform a cold-start initialization of the COMSEC subsystem (HGF-83 (C1-7) in an AN/TYC-39A.
(2) Remember to follow all safety requirements when working with equipment.
(3) You will be provided with the necessary manuals and a copy of the practical exercise to aid you in performing these tasks.
(4) When you feel confident that you can correctly perform cold-start initialization of the TRI-TAC COMSEC subsystem within 45 minutes, ask one of your instructors to evaluate your performance.
(5) If you have no questions, you may start your exercise by reading and following the directions in your practical exercise.
(6) If it is not clear what you are required to do, ask your instructor for clarification.

b. Application to students.

(1) Proceed to the training site when directed by the instructor.

(2) Perform the steps, in sequence, in the application portion of the practical exercise.
(3) Inform the students that if they have any problems with the equipment, ask their instructor for help.

c. Evaluation. Evaluate each student's ability to correctly perform cold-start initialization of the TRI-TAC COMSEC subsystem within 45 minutes.

8H 25M

SUMMARY:

During this lesson, you were shown how to perform a cold-start initialization of the COMSEC subsystem. The importance of this training will become evident as you reach your first TRI-TAC unit and participate in a major exercise.

8H 30M

END

This document supports Task Number 113-603-3205.

U.S. ARMY SIGNAL CENTER AND FORT GORDON
Fort Gordon, Georgia 30905-5180

LESSON PLAN

TITLE: Installing, Loading and Rekeying the (Digital Subscriber Voice Terminal (DSVT) (KY-68)

LEARNING OBJECTIVE:

Action: The student will install, load and rekey the KY-68. The student will also place a secure call with the KY-68 DSVT.

Conditions: The student will be given an operational AN/TYC-39A w/peripherals, KY-68/TSEC, TM 11-5810-292-10, TM 11-5810-329-10, KYK-13 w/cables, KYX-15A w/cables, hook-up wire, and practical exercise.

Standards: Acceptable performance is met when the student correctly installs, loads, and places a secure call with the KY-68 DSVT within 30 minutes.

SAFETY CONSIDERATIONS: There are no safety considerations for this lesson.

RISK ASSESSMENT: Low.

RESOURCE NEEDS/REFERENCES: Operational AN/TYC-39A w/peripherals, KY-68/TSEC, TM 11-5810-292-10, TM 11-5810-329-10, KYK-13 w/cables, KYX-15A w/cables, hook-up wire, practical exercise, overhead projector, slides 1-7, TB 380-40, and JCS Pub 6-05.5 (C).

APPROVAL DATE: 25 NOV 97
DEVELOPER: SFC CARTAGENA
DIV. CHIEF: Jack P. Rondon

METHODS OF
INSTRUCTION: Conference, Demonstration, Practical Exercise.

TIME: 6 Hours

NOTES TO INSTRUCTOR:

1. Ensure all TMs are available prior to class.

2. Ensure that two KYX-15A and/or KIK-13 fill devices w/cables are available prior to class.

3. Ensure the students observe proper safety precautions.

4. Prior to class, set up the equipment to perform the required training objectives.

5. Control and maintain a signout roster to ensure that students sign for required classified training materials.

6. Evaluate students on their ability to perform the learning objective during the practical exercise.

INTRODUCTION:

Elapsed Time

1. The installation of any telephone equipment is important to the user; however, COMSEC equipment has its own specific requirements which must be observed.

2. Because the KY-68 DSVT uses keys, it becomes classified as soon as it is loaded with the keys and must only be made available or accessible to authorized users.

3. During this lesson, we will discuss and perform installation, loading, and rekeying of the KY-68, and perform a manual cooperative key transfer.

5M

BODY

NOTE: Show Slide 1.

1. Purpose and use.

a. The KY-68 is used for encrypting/decrypting voice traffic and provides secure digitized data traffic when used with various devices.

b. Characteristics, capabilities, and features.

(1) Operates as a full-duplex or half-duplex voice/data subscriber terminal.
(2) Handles 16 kilobits per second (kb/s) to 32 kb/s traffic.
(3) Provides secure and nonsecure access to switched networks.
(4) Can be operated with a communications security (COMSEC) parent or COMSEC subordinate switch.
(5) Operates from a common battery or local power source.

QUESTION: What is the purpose of the DSVT TSEC/KY-68? (ANS: The KY-68 is for encryption/decryption voice traffic and provides secure digitized data traffic when used with various devices.)

10M

2. Installation.

a. Connectivity.

(1) The KY-68 is used by a variety of subscribers in a multitude of environments from a foxhole to setting at a desk at a major command headquarters.
(2) They can be directly connected to the AN/TYC-39A TRI-TAC switches via 26-pair cable and a J-1077, a remote multiplexer Combiner (RMC) TD-1234, or a remote loop group multiplexer (RLGM) TD-1233 (P).

NOTE: Show Slides 2 and 3. (RMC and RLGM)

(3) They can also be remotely connected to the previously mentioned equipment, via a transmission system such as digital group multiplexer (DGM) radio, tactical satellite (TACSAT), or TROPOSCATTER.
(4) Regardless of the method used to get the voice path to the phone, the KY-68 will ultimately be connected using four wires between the terminating equipment and the back of the KY-68.

b. Programming.

(1) As with any of the other types of telephone equipment you have been introduced to in previous lessons, the KY-68 must be added to the database to function following the same procedures you have already learned with one minor exception.
(2) Because of the use of keys, care must be taken to check the profile being used for the subscriber and ensure that the subscriber has been provided with the appropriate key.

NOTES: AN/TTC-39A switch operators will also have to make the necessary assignments to match the key locations to the appropriate subscriber directory numbers.

Show Slide 4. (Back of KY-68.)

c. Installation.

(1) Determine which pair of the four wires are going to be used for the transmit (XMT) and which is the receive (RCV).
(2) Connect the XMT pair to the BLK (XMT) connectors and RCV pair to the RED (RCV) connectors.

NOTE: Caution must be exercised as there is a difference in the potential of 56 VDC at 300 mA on the receive pair.

(3) When the KY-68 is mounted in the message switch, power is supplied through an external power connector from the 28-volt DC bus of the switch, and not the XMT and RCV pair.
(4) An external power supply, the HYP-7l, may also be used to supply power for the DSVT when no other source is available. This could occur if the DSVT is at the end of a radio link and there is no digital group multiplexer (DGM) equipment to supply the power.
(5) Sole User Mode.

In this configuration, two KY-68s may be connected point-to-point.

1. The XMT and RCV pairs must be transposed at one end.
2. The same keys loaded into the respective LDU and LDX locations of both phones.
3. Power must be supplied by an external source.
4. When going OFF-HOOK, ringback will be heard.

d. Transferring key to subscriber equipment.

(1) The corresponding key must be withdrawn from the HUS of the HGX-83 (A) and stored in a fill device for transport to the location of the DSVT.

NOTES: Whenever providing keys for subscribers, it is imperative that one of the REA, R, or MSRT versions of the X-TEK is issued in addition to the U-KEK to allow the subscriber to reenter the net if a net rekey has been performed.

Show Slide 5.

Automatic Key Distribution Center Rekeying Control Unit (AKDC).

(2) Transfer a key from the HUS to the fill device using the following procedures:

NOTE: A check of the location can be performed to ensure that a previously used key is not overwritten by setting the MODE switch to OFF CHECK and pressing the INITIATE pushbutton. If the red PARITY INDICATOR light-emitting diode (LED) flashes, a key exists in that location.

(a) Set the ADDRESS select (FILL) switch of the fill device to the position that the key is to be transferred into.
(b) Connect the fill device with a fill cable to the fill port of the AKDC.
(c) Using the thumbwheels of the HGX-83 (A), dial a command "OO57", HUS to fill device.
(d) Turn the FUNCTION knob of the AKDC to CMD.
(e) Push the START pushbutton on the AKDC and observe "57" in the DISPLAY window.
(f) Dial the storage location of the key using the thumbwheels.
(g) Turn the FUNCTION knob of the AKDC to ADRS A.

NOTE: When performing the next step, you MUST press the INITIATE button on the fill device within 7 seconds.

(h) Press and release the START button.
(i) Press the INITIATE pushbutton on the fill device and observe that the PARITY INDICATOR flashes indicating a successful transfer.
(j) Turn the MODE switch to OFF and remove the fill cable from the AKDC.

Question: When you transfer the key to subscriber equipment, where do you obtain the key from? (ANS: The corresponding key must be withdrawn from the HUS of the HGX-83 and stored in a fill device for transport to the location of the DSVT.)

3. Loading, initializing, and operating the DSVT.

a. Loading key.

NOTE: Show Slide 6. (KYK-l3)

(1) With the fill device in the OFF position, connect the fill device with cable to the KY-68s fill connector.
(2) Set the ADDRESS select (FILL) switch of fill device to the position of the key to be loaded into the equipment (U-KEK).

NOTE: A check of the location may be performed to ensure that a good key is in the location.

(3) Set the MODE switch in the ON position.

NOTES: DO NOT press the INITIATE button.

Reshow Slide 1. (KY-68)

(4) Set the KY-68 FUNCTION SEL switch to the LDU position.
(5) Observe the following:

(a) RING/BUSY indicator lites.
(b) NSW indicator lites.

(6) Move the KY-68 spring loaded VAR STOR switch to LOAD and hold. The annunciator will sound one PARITY tone.
(7) Release the VAR STOR switch letting it return to its normal (center) position and a second PARITY tone will be heard indicating a successful load of the U-KEK. You should also be able to observe the PARITY indicator flash on the fill device.

NOTE: If an l-second tone or no tone is heard, the key has not been properly loaded. Return the FUNCTION SEL switch to DSBL and repeat the loading procedure.

(8) Set the fill device ADDRESS select (FILL) switch to the position where the X-TEK is stored.
(9) Set the KY-68 FUNCTION SEL switch to the LDX position.
(10) Observe the following:

(a) RING/BUSY indicator lites.
(b) NSW indicator lites.

(11) Move the VAR STOR switch to LOAD and hold, the annunciator will sound one PARITY tone.
(12) Release the VAR STOR switch and let it return to its center position. The annunciator will sound a second PARITY tone indicating a successful load of the X-TEK. You should also be able to observe the PARITY indicator flash on the fill device.

NOTE: If an l-second tone or no tone is heard, the key has not been properly loaded. Return the FUNCTION SEL switch to DSBL and repeat the loading procedure.

(13) Set the FUNCTION SEL switch to OP; observe that the RING/BUSY and NSW indicators go OFF.
(14) The KY-68 is now loaded.

b. Initializing the KY-68.

(1) Prior to using the DSVT, another factor must be considered, if the phone is in service.
(2) If the KY-68 is OOS, when the subscriber goes OFF-HOOK for the first time after loading, the initial synchronization process fails and appears to be a bad load or faulty KY-68.
(3) If the KY-68 is loaded properly with the U-KEK and the reentry key in the X-TEK positions, when going OFF-HOOK for the first time the following should occur:

(a) A series of synchronization sounds will be heard in the handset of the KY-68.
(b) A minimum of two LKGs will be required to allow for the verification, synchronization and rekeying process to take place. Each DSVT will be rekeyed with its current X-TEK.
(c) The two LKG BUSY lites can be observed flashing in the switch.
(d) Upon successful rekeying of the current X-TEK, the subscriber will receive a dialtone.
(e) This process will take about 30 seconds, be patient.

35M

c. Operating under normal conditions.

(1) Calling modes.

There are three calling modes that are utilized with the KY-68: Secure, secure using "S" or compartmented key, or nonsecure.

1. Secure.

a. Lift the handset and ensure that the HOOK switch is not locked down. (Should normally be unlocked, locked position is for use in the data mode when a handset is not required or when using a headset).
b. After receiving dialtone, dial the number as with any other military phone.
c. The call will be placed to another secure DSVT or MSRT and a secure connection will be made through the network.

d. Once the connection is made, the LKGs will drop out of the connection and the DSVT/MSRTs will secure the call end-to-end.

2. Secure using "S" or compartmented key.

NOTE: Both DSVTs must have a fill device that contains the same "S" key.

a. Establish a normal secure call.

NOTE: Before loading the "S" key, both DSVTs must be in secure end-to-end traffic.

b. Verify that the FUNCTION SEL switch is in the OP position.
c. After all users agree to use the "S" key, each must connect a fill device to their end and set the MODE switch to ON.
d. Set ADDRESS selector (FILL) switch to the "S" key location.
e. Press and hold the "R" key on the KY-68s keypad, then press and release the PUSH-TO-TALK switch on the handset.
f. Release the "R" key.
g. All users now inform each other that they are now ready to load the "S" key.
h. All users simultaneously move the FUNCTION SEL switch to the SVAR position and then back to the OP position to load the "S" key. The switch

is spring loaded and will return automatically.

i. Observe that the RING/ BUSY indicator lites and that the NSW indicator lites.

j. Move the KY-68 VAR STOR switch to LOAD and hold. The annunciator will sound a PARITY tone.

k. Release the KY-68 VAR STOR switch and let it return to its normal (center) position. The annunciator will sound again indicating a successful load of the "S" key.

NOTE: Unless all users have the proper "S" key loaded, NO user can communicate in the "S" key mode.

l. All users must now set their fill device MODE switch to OFF/CK and disconnect the fill device from the KY-68.

NOTE: The "S" key is not stored by the battery in the KY-68 and will be erased if power is lost to the phone during the call.

3. Zeroizing.

a. Whenever you are done with your mission or you must leave the KY-68 unattended, it must be zeroized.

b. To zeroize or erase the stored keys, simply raise the VAR STOR switch slightly and move the ZERO (left) position.

d. Operating under emergency conditions.

(1) Should the KY-68 become zeroized accidentally or during an overrun situation, emergency access to the switch is possible using the following procedure:

(a) Place the HOOKSWITCH in the OFF-HOOK (middle) position. After 10 seconds, the terminal will automatically go into the EMERGENCY ACCESS mode and you will hear the Plain Text Alert tone. Observe the RING/BUSY and NSW indicators lite.

(b) You may also gain emergency access by pressing the "O" button on the keypad as soon as you go OFF-HOOK.

(2) If the KY-68 contains key, but emergency access is desired, gain access by pressing and holding the "O" button on the keypad PRIOR to going OFF-HOOK.

NOTE: All emergency access calls will be in the PLAIN-TEXT mode (nonsecure). CAUTION must be exercised as to the type of information transmitted over the DSVT.

QUESTION: Will emergency access calls be in plain text mode? (ANS: All emergency access calls will be in plain-text mode (nonsecure).)

4. Rekeying the DSVT.

a. Performing a periodic COMSEC net rekey is required, as has been discussed in a previous lesson, to prevent possible compromises from occurring.

b. The procedure is performed using the Assign Net Rekey command (ANR) and is monitored or verified with the Assign Variable Location (AVL) command.

c. Up to 15 COMSEC nets of the same type can be automatically rekeyed using this command.

d. The process obtains a new X key from the KG-83, downloads it into a storage location in the HUS, extracts a copy of it and transfers it to an LKG where it is sent the DSVT. When received at the DSVT, the new X-TEK is overwritten into the DSVT's LDX position.

QUESTION: Why is a period COMSEC net rekey required? (ANS: A period COMSEC net rekey is required to prevent possible compromise from occurring.)

3. Manual cooperative key transfer.

a. This procedure is used to electronically transfer keys from the controlling switch operator's KYX-l5A net control device (NCD) to the receiving switch operator's NCD via KY-68s.

NOTE: Show Slide 7. (KYX-l5A)

b. Cooperating KG-84A/KYX-l5A pairs can also be used for this procedure, if necessary.

c. Transfer procedure.

(1) Each switch operator must have the same pair-wise UIRV (KEK) stored in their KYX-l5A.
(2) The transmitting KY-68 must have the key to be transferred stored in their KYX-l5A.
(3) Operator actions are as follows:

(a) Establish secure end-to-end communications.
(b) The transmitting KY-68 operator must inform the receiving KY-68 operator of the intent to perform the key transfer.
(c) Both KY-68 operators connect their KYX-l5As to the DSVTs fill connector using a fill cable.

(d) The transmitting KY-68 operator sets the ADDRESS select switch of the key to be transferred to ON.

1. Next, move the MODE switch on the KYX-l5A to LD; all other switches should be OFF.
2. Move the VAR STORAGE switch on the KY-68 to the LOAD position and release.
3. Two parity tones will be heard and the PARITY lite on the KYX-l5A flashes.

(e) The transmitting KY-68 operator then sets the ADDRESS select switch of their KYX-l5A's UIRV location to the ON position.

1. Next, place the MODE switch on the KYX l5A in the MK (manual keying) position.
2. All other address select switches should be OFF.

(f) The receiving KY-68 operator sets the ADDRESS select switch of the KYX-l5A for the UIRV to the ON position.

1. Next, place the MODE switch on the KYX-l5A to the LD position.
2. Move the VAR STORAGE switch on the KY-68 to LOAD position.
3. Two parity tones should be heard and the PARITY lite on the KYX-l5A should flash.

(g) The receiving KY-68 operator selects the location for the key to be received by setting the designated ADDRESS select switch to ON.

1. The selected location should be zeroized prior to selection.

2. All other key locations should be OFF.
3. Next, place the MODE switch on the KYX-15A to the RV (receive key) position and push the MODE INITIATE button on the KYX-15A.
4. The transmitting KY-68 receives static in the earpiece and voice communications is temporarily broken.

(h) The transmitting KY-68 operator, upon hearing the static, pushes the MODE INITIATE button on the KYX-15A.

1. After a slight delay, the red PARITY lite on the KYX-15A flashes.
2. Next, place the MODE selector switch on the KYX-15A to OFF/CK.
3. Communications should be reestablished.

(i) After noting the PARITY light flash on the KYX-15A the receiving KY-68 operator does the following:

1. Places the MODE selector switch on the KYX-15A to OFF/CK.
2. Presses the MODE INITIATE button on the KYX-15A.
3. The PARITY lite should flash again, indicating a successful transfer.

(j) After completing the transfer(s), ensure that the KYX-15As are in the OFF/CK position and remove them from both KY-68s.

QUESTION: What is the Manual Cooperative Key Transfer used for? (ANS: The Manual Cooperative Key Transfer is used to electronically transfer keys from the controlling switch operator’s KYX-15A Net Control Device (NCD) to the receiving MS switch operator's NCD via KY-68s.

1H 30M

4. Demonstration.

a. Demonstrate installing a KY-68.

b. Loading Key into a KY-68.

c. Place a secure call using a KY-68

2H

5. Practical exercise.

NOTES: During the practical exercise, observe the students on their ability to perform the learning objective; coach, if necessary.

Have two students work together on equipment during the practical exercise. Students awaiting or having completed hands-on training will review their notes.

a. Explanation to students.

(1) During this practical exercise, you will perform the following tasks:

(a) Install a KY-68.
(b) Load key into a KY-68.
(c) Place a secure call using a KY-68.

(2) When you feel confident that you can correctly install, load, and place a secure call using a KY-68 (DSVT) within 30 minutes. Ask one of your instructors to evaluate your performance.
(3) If it is not clear what you are required to do, ask your instructor for clarification.

b. Application to students.

(1) Proceed to the training area when directed by your instructor.
(2) Perform the steps as they are sequenced in the application portion of the practical exercise.

(3) You will use your TMs to perform each individual step.

c. Evaluation. Evaluate each student's ability to correctly install, load, and place a secure call using the KY-68 DSVT within 30 minutes.

5H 55M

SUMMARY

During this lesson, you were provided an opportunity to install, load, and operate a KY-68.

All of these things must be second nature to a 74G and will be a large part of your daily routine in the field.

6H

END

This document supports Task Number 113-603-3205.

U.S. ARMY SIGNAL CENTER AND FORT GORDON
Fort Gordon, Georgia 30905-5180

LESSON PLAN

TITLE: Trunk Encryption Device

LEARNING OBJECTIVE:

Action: The student will patch or configure a TED for operation, perform a cold-start initialization, change variable and local update of the KG-94 TED.

Conditions: The student will be given an operational AN/TYC-39A with a populated communications security (COMSEC) rack and TM 11-5805-790-12 series (39A) and TM 11-5810-361-10.

Standards: Acceptable performance in Part One is achieved when the student correctly performs a cold-start initialization, change variable and local update of the KG-94 within 45 minutes. Acceptable performance in Part Two is achieved when the student correctly answers 14 of 20 written questions in 1 hour.

SAFETY CONSIDERATIONS: There are no safety considerations for this lesson.

RISK ASSESSMENT: Low.

RESOURCE NEEDS/ REFERENCES: AN/TYC-39A with a populated communications security (COMSEC) rack, TM 11-5805-790-12 series (39A), TM 11-5810-361-10.series, overhead projector, slides 1-2, fill device with cable, and KAO-l93A (C).

APPROVAL DATE: 25 NOV 97
DEVELOPER: SFC CARTAGENA
DIV. CHIEF: Jack P. Rondon

METHODS OF
INSTRUCTION: Conference, Demonstration, Practical Exercise.

TIME: 4 Hours

NOTES TO INSTRUCTOR:

1. Ensure all required TMs are available prior to class.

2. Ensure the students observe proper safety precautions.

3. Ensure that a minimum of two TEDs are available in the switch.

4. Ensure that all necessary patch cords and/or CX-ll23O cable are on-hand to patch the two TEDs back-to-back if only one switch is available.

5. The reduction in time reflects the reduced student input for RC classes and is to be taken from PEl time.

INTRODUCTION:

Elapsed Time

1. During previous classes, you were introduced to the various components that are involved with the encryption and decryption of individual subscriber voice and data traffic.

2. This lesson will focus on the piece of equipment that the switch uses to encrypt/decrypt all of the information passed over a digital transmission group (DTG) in bulk. This form of encryption is commonly known as "bulk" encryption.

3. Because the TYC-39A and family of switches rely on their ability to provide secure communications for their subscribers, it is imperative that you have a thorough understanding of how to use the trunk encryption devices (TEDs).

2M

BODY:

1. Connectivity.

a. Message switch (MS) AN/TYC-39A.

(1) In MS applications, the TEDs are dedicated to the time division interface group (TDIG) that is on-line.

(a) The MS has two redundant TDIGs, only one of which is on-line at a time.
(b) A third TED is located in the HGF-83 which is present only as a spare should either of the dedicated TEDs becomes inoperable.

The TED 3 must be physically removed from its storage slot and installed into the required TED position.

(2) Using patching techniques, TED 1 could be substituted for TED 2 or visa versa should one of those slots become defective.

b. Network Applications.

(1) The basic rule for trunk encryption is that an even number of TEDs must be utilized in a transmission path, end-to-end.

NOTE: Show Slide 1 (TED Network Configurations).

(2) The TEDs may be housed in the switch, or in an immediate adjacent radio terminal, but must be somewhere at the beginning and end of the transmission path.

QUESTION: What purpose does patching a TED serve when it can be utilized without any patches? (ANS: Allows the operator the ability to patch around faulty equipment or DTGs which are not hardwired for TEDs.)

22M

2. Cold start procedures.

NOTE: Show Slide 2. (TED Faceplate.)

a. Power initialization

When initializing a TED from the powered down (cold start) state, certain steps must be performed in a specified order.

NOTES: Refer students to TM 11-5810-361-10, para 2-7.

Those items listed below assume that proper preventive maintenance checks and services (PMCS) has been performed and the TEDs are functioning properly.

(1) Zeroize the TED by placing the POWER switch to the ZEROIZE/OFF position.
(2) Ensure that a fill battery is installed and the date is current (within 180 days).
(3) Set POWER switch to ON. The UPDATE counter should read "OO" and the POWER ON (green) and ALARM (red) lights should be on.

NOTE: Refer students to para 2-8.

b. Load the KG-94 with a key.

(1) Using a fill cable, connect a fill device to the KG-94 that contains the proper TED key.
(2) Ensure the fill device is ON and the ADDRESS SELECT switch is in the proper position.
(3) Turn the KG-94s FUNCTION SELECT switch to LOAD.
(4) Press the ACTUATE button momentarily. The PARITY light should light indicating a successful load. The ALARM and POWER ON lights should stay ON.

NOTE: The ALARM light stays ON until the TED obtains synchronization with another TED or itself when in loopback.

(5) Returning the FUNCTION SELECT switch to the LAMP TEST position after any operation assures that an accidental push of the ACTUATE button will cause no unwanted results.
(6) It has become a field standard to immediately perform a Change Key operation prior to passing traffic.

c. Perform a Change Key operation.

NOTE: This must be performed at BOTH ends of the system.

(1) Once the TEDs are properly loaded with key, the following steps must be performed to achieve synchronization and ensure a secure path for communications.

(a) Turn the FUNCTION SELECT switch to CHNG KEY and momentarily press the ACTUATE button.
(b) When the local TED is connected in-system to another TED (or in loopback) which is loaded with the same key, the following occurs:

1. The PARITY light goes out.
2. The ALARM light goes out.
3. The number "0l" appears in the UPDATE window.
4. The RESYNC light lights to indicate TEDs are in-sync end-to-end.
5. The FULL OPR light lights to indicate the TED is operational.

(2) If the Change Key operation was unsuccessful, only the PWR ON and OLD KEY lights will be on and the UPDATE

window will be blank or not have advanced. If this occurs, perform the following steps:

a. The initiator of the CHNG KEY should turn the FUNCTION SELECT switch to RESTART and press the ACTUATE button.

   Only the PWR ON and OLD KEY lights should be on.

b. The other end should turn their TED's FUNCTION SELECT switch to RESTART and press the ACTUATE button.

   (1) The path should be restored using the old TEK.
   (2) The PWR ON, RESYNC, and OLD KEY lights should be on.

c. Repeat the updating procedure, if it fails again and you are sure that all steps were performed correctly, replace the TEDs.

(3) A Change Key operation is also performed at the end of each 24-hour period to ensure continued communications.

   a. Each time it is performed, the number in the UPDATE window is advanced by 01.
   b. The controlling switch will perform the 24-hour periodic operations.
   c. When initiated at the controlling switch, the distant end KG-94 acts as a

remote unit and "follows" the actions of the initiating unit (this can be observed during the demonstration).

A limit of 45 change key operations are authorized for each seed key.

QUESTIONS: What is the recommended life of the fill battery? (ANS: 180 days.)

What number should be in the UPDATE window immediately after completing the cold start procedures and before passing traffic? (ANS: "0l")

42M

3. Local updates.

NOTE: Refer students to para 2-14.

a. Local updates are performed under two circumstances, when replacing a faulty TED or when the TED at one end of the system has been accidentally zeroized.

b. The procedure allows one of the TEDs to "update" itself to the state (level) of the functioning TED.

c. The operator performing the local update must contact the other end and obtain the number in the UPDATE window of the "normal" TED.

d. Upon verification of the number and the seed key used at the beginning of this sequence, the following steps must be performed:

(1) Place the POWER switch in the ON position, the PWR ON and ALARM lights should light.
(2) Load the KG-94 with the original seed TEK used for the current sequence of Change Key operations.

(3) Set the FUNCTION SELECT switch to the LCL UPDATE position.
(4) Press the ACTUATE button the amount of times required to advance the number in the UPDATE window until equal to that of the functional TED.
(5) When both TEDs have the same number showing in the UPDATE window, the RESYNC and FULL OPR lights should light and communications restored.

QUESTIONS: When is a loca1 update performed? (ANS : When replacing a faulty TED or when a TED has been accidentally zeroized.)

What is the primary difference between a Change Key operation and a local update operation? (ANS: Change key creates a new permutation of the seed key on a periodic basis vs local update which brings one TED in a system up to the permutation level of the operational TED.)

5OM

4. Loss of synchronization.

a. Loss of synchronization between TEDs in a network sometimes occurs when the transmission system encounters a loss of signal for various reasons.

b. The TEDs may regain synchronization without intervention. If they do not, follow similar procedures that were used in the initial Change Key operation:

(1) The operator at one end of the path should turn the FUNCTION SELECT switch to RESTART and press the ACTUATE button.

(a) The PWR ON, RESYNC, and FULL OPR lights should be on.
(b) If this is unsuccessful, have the other end operator do the same procedure.

(2) The other end should turn their TED's FUNCTION SELECT switch to RESTART and press the ACTUATE button.

(a) The path should be restored.
(b) The PWR ON, RESYNC, and FULL OPR lights should be on.

(3) This procedure has been referred to in the field as "bumping" the TEDs.

(4) If this fails, ensure that the same TEK has been loaded into both TEDs and that both are on the same update (same number appears in the UPDATE window).
(5) As the final resort, change the TEDs.

1H

5. Demonstration.

a. Demonstrate initializing a KG-94.

b. Loading key into a KG-94.

c. Performing key change.

d. Performing local update.

1H 30M

6. Practical exercise.

NOTES: During the practical exercise, observe the students on their ability to perform the learning objective; coach, if necessary.

Have two students work together on equipment during the practical exercise. Those students waiting their turn in the lab will answer written questions in Part Two of the practical exercise.

a. Explanation to students.

(1) During this practical exercise, you will perform the following tasks:

a. Demonstrate initializing a KG-94.
b. Loading key into a KG-94.
c. Performing key change.
d. Performing local update.

(2) When you feel confident that you can correctly initialize, load, perform key change, and perform local update to the KG-94 (TED) within 45 minutes. Ask one of your instructors to evaluate your performance.
(3) If it is not clear what you are required to do, ask your instructor for clarification.

b. Application to students.

(1) Proceed to the training area when directed by your instructor.
(2) Perform the steps as they are sequenced in the application portion of the practical exercise.
(3) You will use your TMs to perform each individual step.

c. Evaluation. Evaluate each student's ability to correctly initialize, load, perform key change, and perform local update to the KG-94 (TED) within 45 minutes.

3H 58M

SUMMARY:

During this lesson, you had an opportunity to patch or configure a TED and prepare it for operation in a new or existing network. You also were introduced to techniques used in the field to restore synchronization of the TEDs in an existing system. This information will enhance your ability to perform your daily duties in the field.

4 H

END

This document supports Task Number 113-603-3205.